73rd MORSS CD Cover Page

712CD

For office use only 41205

UNCLASSIFIED DISCLOSURE FORM CD Presentation

21-23 June 2005, at US Military Academy, West Point, NY

Please complete this form 712CD as your cover page to your electronic briefing submission to the MORSS CD. Do not fax to the MORS office.

Author Request **(To be completed by applicant) - The following author(s) request authority to disclose the following presentation in the MORSS Final Report, for inclusion on the MORSS CD and/or posting on the MORS web site.**

Name of Principal Author and all other author(s):

Principal Author: Mr. Richard Jodoin
Threat Systems Management Office

Other Author's: Mr. Paul D. Kelley/ ATEC and
Mr. Emanuel M. Tornquist/ Northrop Grumman IT - TASC

Principal Author's Organization and address:

Threat Systems Management Office
Attn: SFAE-STRI-PMITTS-S/Jodoin
Redstone Arsenal, AL 35898-7461

Phone: **(256) 876-8614**

Fax: **(256) 876-0314**

Email: ***richard.jodoin@us.army.mil***

Original title on 712 A/B: ***Synthetic Jammer in Seamless and Interactive Environments: A Study and Demonstration***

Revised title: ***Synthetic Jammer in Seamless and Interactive Environments: A Study and Demonstration***

Presented in (input and Bold one): (WG **07**, CG___, Special Session ___, Poster, Demo, or Tutorial):

This presentation is believed to be:
UNCLASSIFIED AND APPROVED FOR PUBLIC RELEASE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 JUN 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Synthetic Jammer in Seamless and Interactive Environments:A Study and Demonstration	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army Test & Evaluation CommandTest and Technology Directorate4501 Ford Avenue, Suite 790Alexandria, VA 22302**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM201946, Military Operations Research Society Symposium (73rd) Held in West Point, NY on 21-23 June 2005. , The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**18**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

73rd MORS Symposium

Synthetic Jammer in Seamless and Interactive Environments: A Study and Demonstration

Mr. Paul D. Kelley
US Army Test & Evaluation Command
Test and Technology Directorate
4501 Ford Avenue, Suite 790
Alexandria, VA 22302
Voice (703) 681-4887
Fax (703) 681-6914
paul.d.kelley@atec.army.mil

Mr. Richard Jodoin
Threat Systems Management Office
Attn: SFAE-STRI-PMITTS-S/Jodoin
Redstone Arsenal, AL 35898-7461
Voice (256) 876-8614
Fax (256) 876-0314
richard.jodoin@us.army.mil

Emanuel M. Tornquist
Northrop Grumman IT - TASC
600 Boulevard South, Suite 201
Huntsville, AL 35802
Voice (256) 213-5461
Fax (256) 883-0212
emanuel.tornquist@ngc.com

Agenda

- Background
- Problem Statement
- Objectives
- Approach
- Methodology
- Issues
- End State
- Conclusion

Background

U.S. Army Test and Evaluation (T&E) is facing several complex and challenging issues:

- ***Unrealistic Threat Environment* – *Current threat representations do not provide a dynamic and free thinking threat that can act against and react to Blue systems and forces under test, especially in the key areas of Electronic Warfare (EW) and Information Operations (IO)***
- ***Disconnect Across Simulation Domains* – *No approach currently exists to support a realistic threat environment within the constructive domain that will adequately augment the live and virtual components of T&E***
- ***Real Time Casualty Assessment (RTCA)* – *Current RTCA models and systems do not support real-time or near real-time feedback and assessment of Blue and threat force dynamic interchanges during T&E***
- ***Range Restrictions* – *Many DoD test ranges preclude open air RF jamming; federal restrictions such as safety issues with regard to GPS jamming***
- ***Resource Challenges* – *Availability of military units to participate in test events; simply can't fit a Unit of Action (UofA) or Unit of Employment (UofE) on existing test ranges***

Problem Statement

- ***BECAUSE** the live, virtual, and constructive arenas continue to merge into a cohesive environment for the support of testing and training, it is critical that threat realism, as related to EW and IO, is able to transition across all three domains;*

- ***THERE EXISTS AN IMMEDIATE NEED** for Electronic Attack (EA) models which support EW within the constructive testing environment and which will augment the live and virtual components of T&E;*

- ***AND** we need to integrate this capability in a manner that provides seamless interoperability across the simulation domains*

Problem Statement

- ***IS IT POSSIBLE* to link the U.S. Army Test & Evaluation Command's (ATEC) and Threat Systems Management Office's (TSMO) existing and planned EW assets with simulation to provide a synthetic environment for testing Network Centric Battlefield Systems?**

- ***IF YES,* then which simulations should be considered and how should the different assets and systems be linked across the simulation domains?**

Objectives

- **Conduct a study with emphasis on the "science" of modeling for EA and the resulting recommendation of how to "fix" Modeling and Simulation (M&S) of jamming**
  - ***Threat Roadmap* – *the development of a threat roadmap to provide a plan of how to achieve the threat acquisition, maintenance, and planning needed to meet Operational Testing (OT) requirements***
  - ***EA M&S Implementation* – *a recommendation for implementing an adequate representation of jamming in the constructive, or M&S, domain; and, an approach to interfacing the M&S implementation with the live domain in a seamless and interactive manner***
- **Use the study as a basis to demonstrate how jamming can be adequately represented in the constructive domain and also serve as a hook into the live domain – providing a cross-domain seamless, interoperable capability**

Approach

- **Conduct a trade study to assess TSMO's capability to provide a threat environment across all three domains that will support EW test requirements**
- **Identify the current end state of a threat EW environment for testing**
- **Identify threat EW M&S capabilities within other Services, DoD, and commercial environments**
- **Produce a Roadmap for implementing a threat EW environment through a block approach**
- **Develop a phased EW testbed demonstration capability**
- **The initial, Phase 1, demonstration of a threat EW representation will implement:**
  - ***Semi-Automated Forces (SAF) and representative Threat Electronic Battlespace components***
  - ***An EW entity in the constructive domain to serve as a "hook" into the live environment***

Methodology

- **Plan**
  - ***Collect, assemble, and analyze information from appropriate sources***
  - ***Engage T&E community in focus groups and workshops to assist core study team to develop, correlate, and evaluate insights and to scope demonstrations***
  - ***Implement Phase 1 Proof of Concept Demonstration Capability***

- **Major Tasks**
  - ***Define needed capabilities, characteristics and metrics***
  - ***Survey on-going programs and initiatives***
  - ***Survey supporting network options***
  - ***Survey supporting modeling and simulation options***
  - ***Identify Usability, Inter-Operability, Gaps, Mobility, Scalability***
  - ***Formulate strategy and implementation alternatives***
  - ***Identify Components for Testbed Demonstration***
  - ***Integrate Phase 1 of Testbed Demonstration***
  - ***Provide Demonstrations of identified capabilities***
  - ***Build the roadmap in compartmented implementation design (staged)***

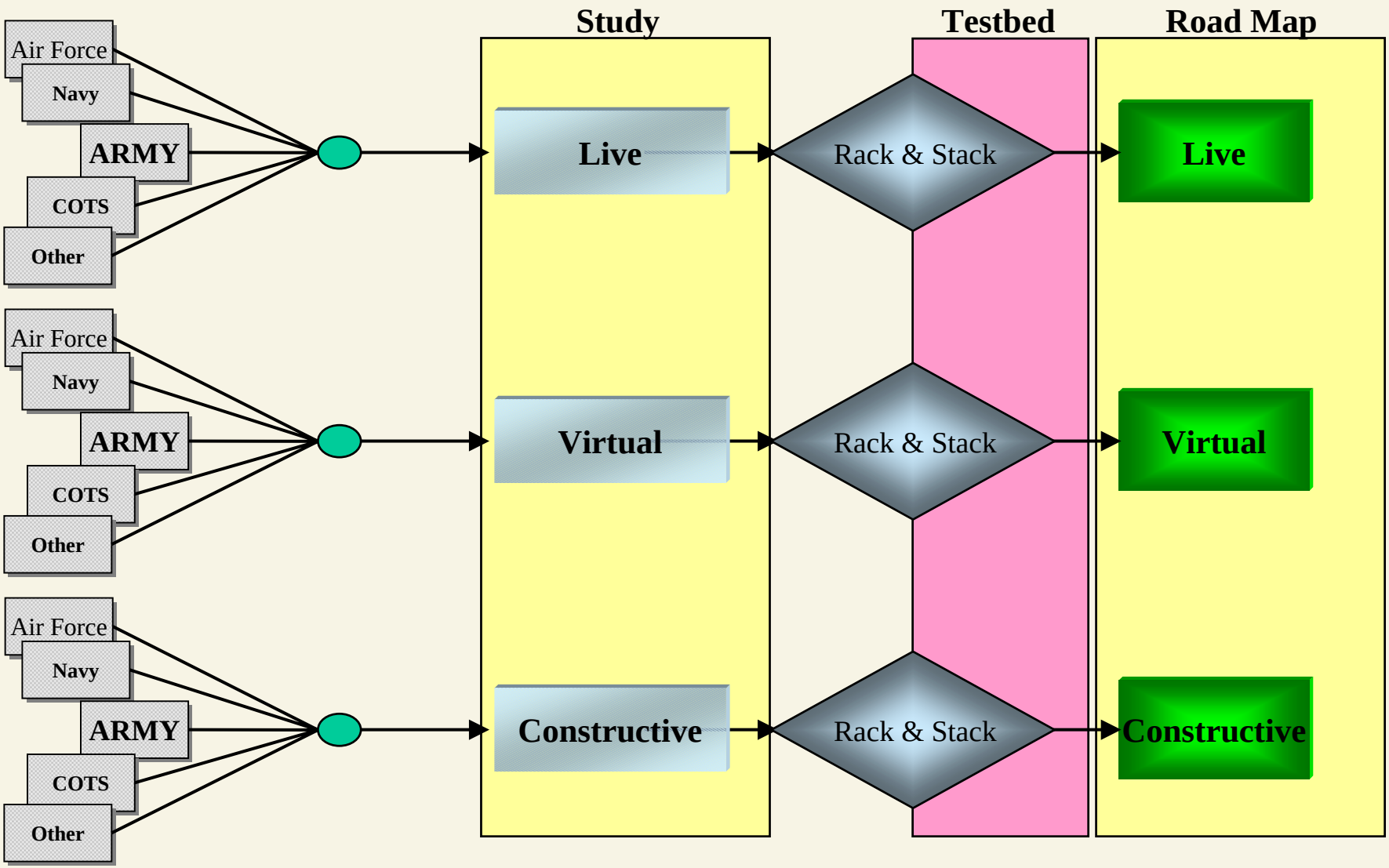
Issues

- ***Communication protocols between live, virtual, and constructive domains that will support jamming and instrumentation requirements for Warfighter Information Network-Tactical (WIN-T) and Future Combat System (FCS)***

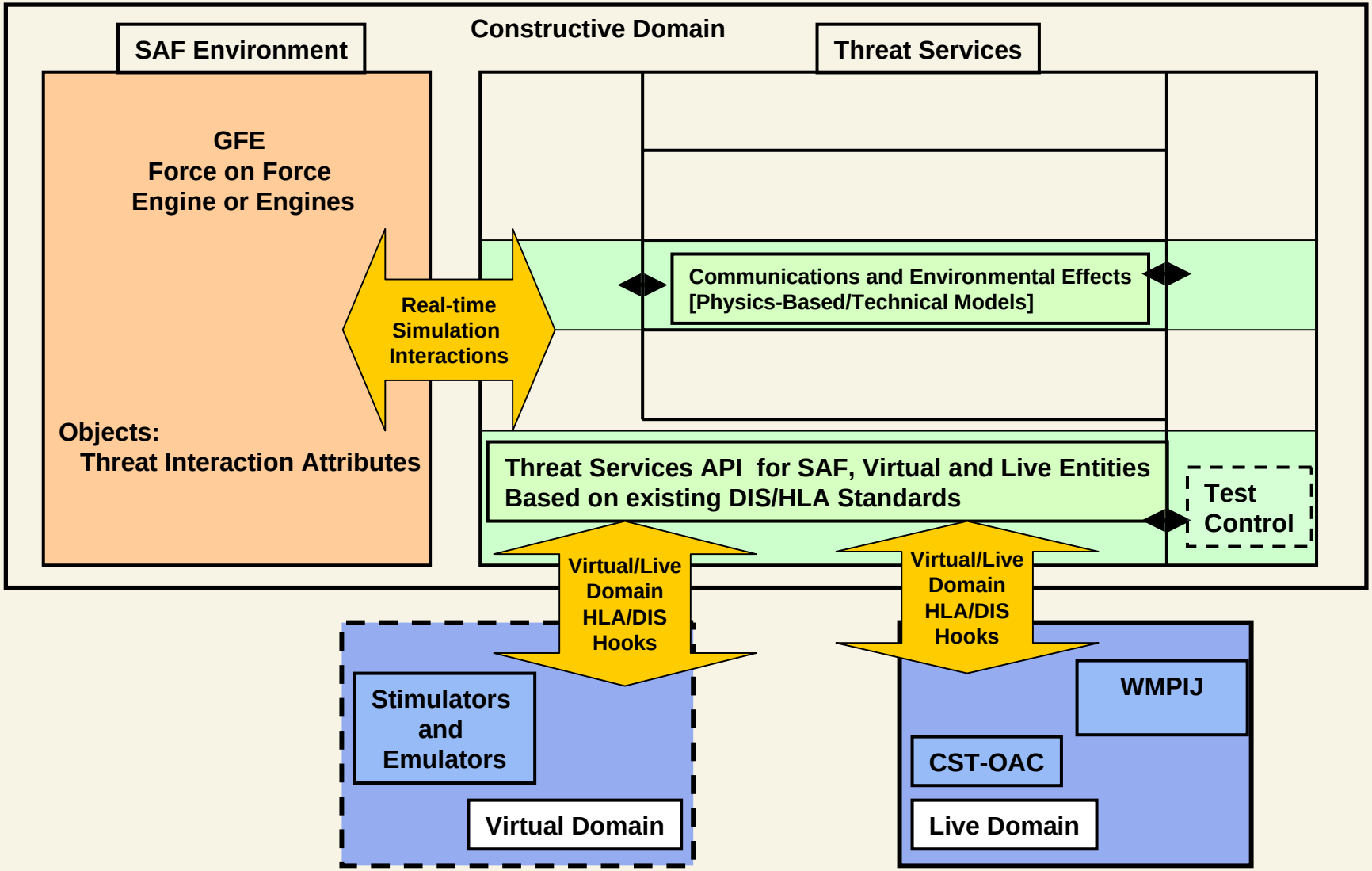
- ***Legacy and evolving architectures and services, how they are currently used and to what effect within their own domain, and how they might be leveraged to provide cross-domain support***

  - ***Distributed Interactive Simulation (DIS)***
  - ***High Level Architecture (HLA)***
  - ***Test and Training Enabling Architecture (TENA)***
  - ***Net Centric Enterprise Services (NCES)***

Study/Testbed Demonstration Architectures



EW Testbed Demonstration – Phase 1



Support of the Live Simulation Domain

Wideband Man Portable Injection Jammer (WMPIJ)

The WMPIJ is a high-fidelity, miniaturized, low-power injection jammer with a frequency coverage from 20 to 1210 MHz that contains components giving it the following operational capabilities:

- **Wideband Receiver Card:**
  - ***Receiver to switch and sample up to 10 different control tones per second***
  - ***Capable of simulating 10 Control Signal Transmitters representing four different simultaneous threat systems***

- **Jamming Waveform Card:**
  - ***An arbitrary waveform (generation of a waveform of the user's choosing) with an instantaneous bandwidth of up to 250 MHz***
  - ***Frequency translation circuit allows the arbitrary waveform to be placed anywhere within the 20 to 1210 MHz band***

Support of the Live Simulation Domain

Control Signal Transmitter and Open Air Capability (CST-OAC)

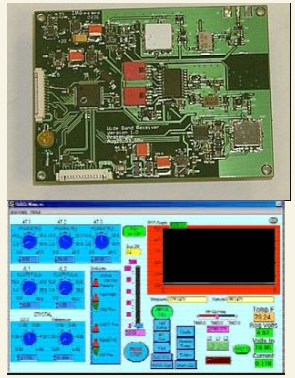
The CST-OAC will:

- ***Leverage previously developed WMPIJ capability***
- ***Allow placement of both small fixed and mobile CSTs where the actual jammers would be***
- ***Be TENA compliant to allow the devices to operate over existing range infrastructure***
- ***Be capable of supporting test, training, requirements analysis, and emerging waveform analysis***
- ***Incorporate both an open air RF signal as well as the receive antenna of the radio, or device under test (DUT), within the environment in which it operates***
- ***Be capable of adjusting absolute power to 1 dB over a very large range, with the final range to be determined after investigation of the threat systems to be replicated***

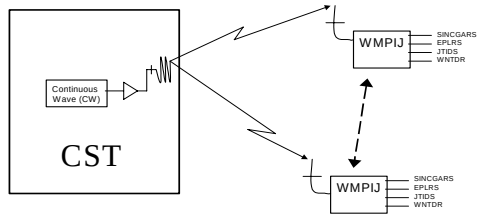
In addition to range scaling, emerging threats with new antenna patterns or polarization can be identified, and the physical antenna used with the CST-OAC changed to factor in different effects of polarization

Study

Demonstration



Live

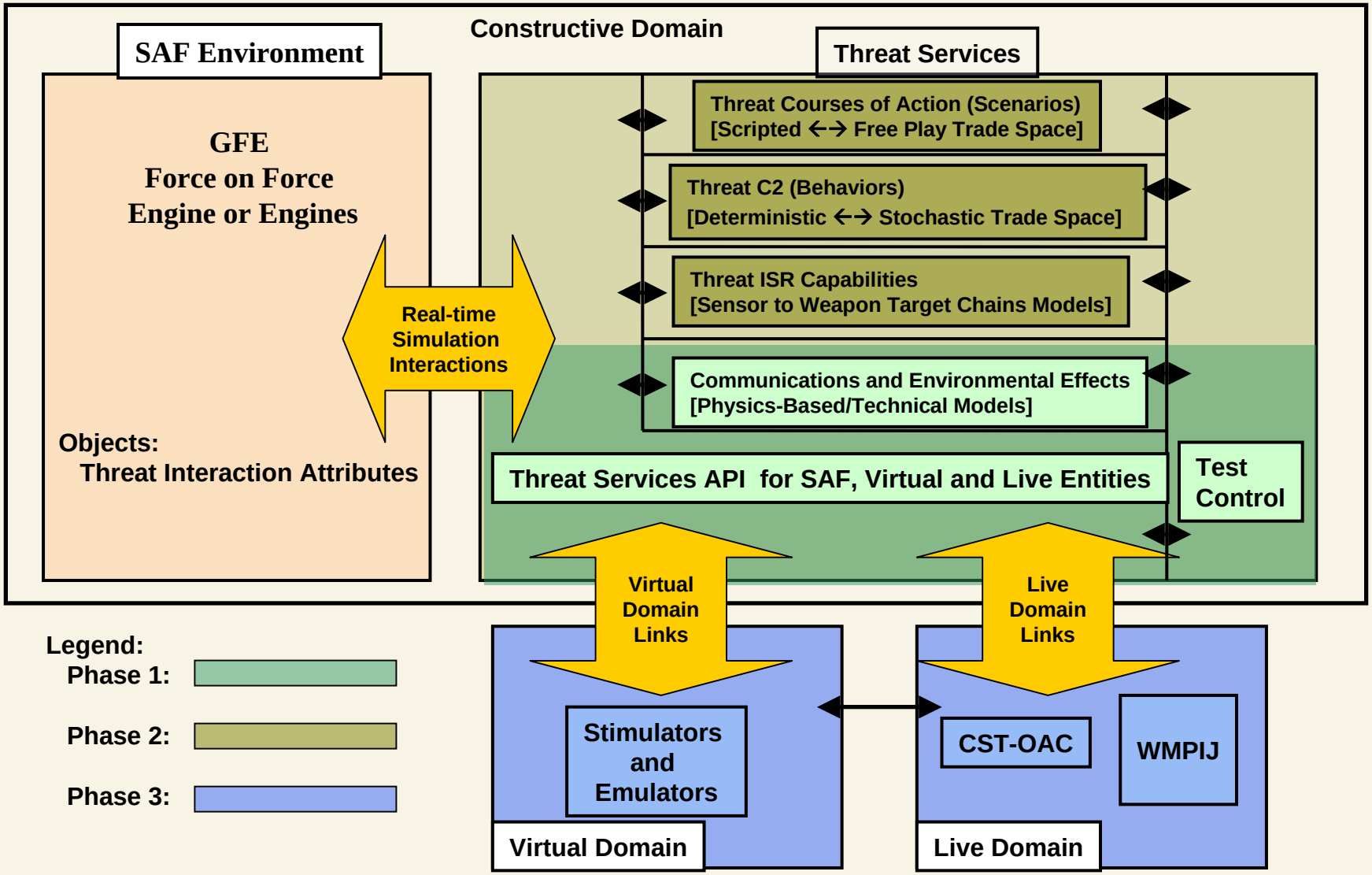


Study & Demonstration Overview

SAF Environment

Constructive EW Entity

EW Testbed Demonstration
High Level View (Phases 1, 2, & 3)



End State

- **Trade Study**
- **Testbed Demonstration Software**
- **Demonstrations of Testbed Capabilities (End-to-End Thread)**
- **Documentation**
  - ***Testbed Demonstration Architecture (OV-1, SV-6)***
  - ***IEW Roadmap***
  - ***Future Direction for Phases 2 & 3***

Conclusion

As the live, virtual, and constructive arenas continue to merge into a cohesive environment for the support of testing and training, it is critical that threat realism of EW and IO is able to transition across these simulation environments

This Study and Demonstration of the seamless integration of a synthetic jammer across interactive simulation environments will provide tangible results in the advancement toward this goal and provide a critical asset for the T&E and Training communities